

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re PATENT APPLICATION of
Inventor(s): RELANDER et al.

Appln. No.: 09
Series Code ↑ Serial No. ↑

Group Art Unit: Not Yet Assigned

2

Filed: November 27, 2001

Examiner: Not Yet Assigned

Title: MAINTAINING END-TO-END SYNCHRONIZATION ON A
TELECOMMUNICATIONS CONNECTION

Atty. Dkt. P 282888 | 2000937US/LT/HER
M# Client Ref

Date: November 27, 2001

**SUBMISSION OF PRIORITY
DOCUMENT IN ACCORDANCE
WITH THE REQUIREMENTS OF RULE 55**

Hon. Asst Commissioner of Patents
Washington, D.C. 20231

Sir:

Please accept the enclosed certified copy(ies) of the respective foreign application(s) listed below for which benefit under 35 U.S.C. 119/365 has been previously claimed in the subject application and if not is hereby claimed.

<u>Application No.</u>	<u>Country of Origin</u>	<u>Filed</u>
20002608	FINLAND	November 28, 2000

Respectfully submitted,

Pillsbury Winthrop LLP
Intellectual Property Group

1600 Tysons Boulevard
McLean, VA 22102
Tel: (703) 905-2000

Atty/Sec: CHM/JRH

By Atty: Christine H. McCarthy

Sig:

Reg. No. 41844

Fax: (703) 905-2500
Tel: (703) 905-2143

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 27.9.2001

jc872 U.S. PRO
09/993947
11/27/01

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

~~2~~



Hakija
Applicant

Nokia Networks Oy
Helsinki

Patenttihakemus nro
Patent application no

20002608

Tekemispäivä
Filing date

28.11.2000

Kansainvälinen luokka
International class

H04L

Keksinnön nimitys
Title of invention

"Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttiyaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.


Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5328
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5328
FIN-00101 Helsinki, FINLAND

Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä

Keksinnön tausta

Keksintö liittyy menetelmään ja laitteeseen päästä-päähän - tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä.

Tietoliikennejärjestelmissä kuten viranomaisverkossa on erittäin tärkeää, ettei liikenteen salakuuntelu ole mahdollista. Ilmatierajapinta on tyypillisesti salattu, joten vaikka radioliikennettä valvotaan, ulkopuolinen ei pysty purkamaan sitä. Infrastruktuurissa liikennettä ei kuitenkaan välttämättä salata, joten liikenne kuten puhe voidaan purkaa käyttäen kyseisen järjestelmän koodekkia. Vaikka ulkopuolinen ei periaatteessa pysty kuuntelemaan puhevuota infrastruktuurin sisältä, tämä on kuitenkin vaativimmille käyttäjille mahdollinen turvallisuusriski. Siksi on kehitetty ratkaisu, jossa puhe voidaan salata päästä-päähän -salauksella. Esimerkkinä päästä-päähän -salauksen mahdollistavasta järjestelmästä on TETRA-järjestelmä (TErrestrial TRunked RAdio).

Päästä-päähän -salauksen perusajatuksena on se, että verkon käyttäjä kuten viranomaisorganisaatio suorittaa liikenteen salauksen ja salauksen purun itsenäisesti ja käytettävästä siirtoverkosta riippumattomasti esimerkiksi päätelaitteiden yhteydessä.

Esimerkiksi TETRA-järjestelmässä päästä-päähän -salausta käytettäessä lähettäjä koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte. Lähettävä päätelaite luo tiettyä avainsarjaa käyttäen salatun näytteen. Salattu näyte lähetetään sitten verkolle. Vastaanottaja purkaa salatun näytteen käyttämällä samaa avainsarjaa, jolloin saadaan taas selväkielinen näyte.

Salauksen murtamisen ehkäisemiseksi avainsarjaa muutetaan jatkuvasti, joten jokainen 60 ms:n ääninäytteen käsittävä kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien on siis sovittava siitä, mitä avainsarjaa on käytettävä jokaiselle kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

Avainsarjakehitin luo avainsarjan tietyn avaimen ja alustusvektorin perusteella. Avaimet jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti. Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen

salausalgoritmi päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salausten murtamisen ehkäisemiseksi.

Tahdistusohjauksen tehtävä on varmistaa, että molemmat päät tietävät, millä alustusvektorilla kukin kehys on salattu. Jotta salaja ja avaaja pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa
5 lähetetään tahdistusvektori. Joskus kyseessä saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikanakin. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti esimerkiksi 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-
10 virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden. Vastaanottaja laskee siis kuinka monta kehystä on lähetetty tahdistusvektorin jälkeen ja avainsarjakehitin luo uuden alustusvektorin viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella.

Tiedonsiirtoverkko saattaa käsittää yhden tai useampia pakettikytkettyjä yhteyksiä, esimerkiksi IP (Internet Protocol) -yhteyksiä, joissa tieto siirretään esimerkiksi IP-puhetekniikalla (voice over IP, VoIP). Eräs standardiprotokolla tosiaikaisen tiedon kuten äänen ja videokuvan siirtämiseen esimerkiksi IP-verkossa on RTP (Real Time Protocol). IP-verkko aiheuttaa tyypillisesti vaihtelevan viiveen pakettien siirrossa. Esimerkiksi puheen ymmärrettävyyden
15 kannalta viiveen vaihtelu on hyvin haitallista. Tämän korvaamiseksi RTP siirron vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja toistaa ne tiettyyn toistoaikaan. Ennen toistohetkeä tullut paketti osallistuu alkuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut paketti on käyttämätön ja hylätty.

Tosiaikainen sovellus vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halutaan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan pakettien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistoviiveen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Useimmilla RTP-algoritmeilla on toiminne, joka
20 säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi. Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että IP-yhdyskäytävä luo 60 ms:n korvaavan paketin. Toisin sanoen lisätään siirrettävän kehysvuon sisälle ylimääräinen kehys.

Ongelmana yllä kuvatussa järjestelyssä on se, että jos käytetään
35 tahdistettua päästä-päähän -salauskooodausta ja kehysvuohon lisätään ylimääräinen kehys, on tämän seurauksena vastaanottopään kehyslaskuri yhden ke-

hyksen etuajassa verrattuna tuleviin kehyksiin eikä vastaanottopään avainsarja enää vastaa lähetyspään avainsarjaa.

Toistoviiveen kasvattamisella esimerkiksi puheenvuoron keskellä on siis se seuraus, että päästä-päähän -tahdistus menetetään, eikä salattu puhe ole enää dekodattavissa. Tämä jatkuu kunnes lähetyspää lähettää uuden tahdistusvektorin, joka tahdistaa vastaanottopään. Tämä ilmiö voidaan välttää siten, että esimerkiksi semidupleksipuheluissa toistoviivettä vaihdetaan vain puheenvuorojen jälkeen. Jos puheenvuorot ovat pitkiä, voidaan toistoviivettä tällöin muuttaa epäedullisen harvoin: puheenlaatu saattaa olla huono koko puheenvuoron loppuun asti, koska toistoviivettä ei voida vaihtaa aiemmin. Edelleen esimerkiksi duplexipuheluissa, joissa ei ole puheenvuoroja ja joissa päätelaite lähettää jatkuvasti, toistoviivettä ei voida vaihtaa ollenkaan koko puhelun aikana, jos halutaan välttää tahdistuksen menetys.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että yllä mainitut ongelmat saadaan ratkaistua. Keksinnön tavoite saavutetaan menetelmällä ja järjestelmällä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa 1, 7, 13 ja 22. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että jos toistoviivettä kasvatetaan tiedon lähetyksen kuten puheenvuoron tai puhelun aikana, merkitään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi ja lasketaan vastaanottopäässä vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset, jolloin toistoviiveen kasvattamiseksi lisätyt ylimääräiset kehykset eivät sekoita päästä-päähän -salauksessa käytettävää kehyslaskuria ja tiedon salauksen purkuun ja siten dekodaukseen ei tule aukkoja.

Keksinnön mukaisen menetelmän ja järjestelmän etuna on se, että ne mahdollistavat toistoviiveen kasvattamisen myös tiedon lähetyksen aikana ilman, että tämän seurauksena salatun tiedon dekodaus häiriintyisi.

Kuvien lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää lohkokaaavion TETRA-järjestelmän rakenteesta;

Kuvio 2 esittää lohkokaaavion päästä-päähän -salauksen toiminnasta;

Kuvio 3 esittää vastaanottajan suorittamaa alustusvektorin laske-
mista;

5 Kuvio 4 esittää kaavion RTP-paketin rakenteesta;

Kuvio 5 esittää RTP-algoritmin toimintaa;

Kuvio 6 esittää kaavion RTP-pakettien tulotodennäköisyydestä siir-
toajan funktiona ja

Kuvio 7 esittää kaavion toistoviiveen kasvattamisesta.

10 Keksinnön yksityiskohtainen selostus

Keksintöä on seuraavassa kuvattu esimerkinomaisesti TETRA-järjestelmän yhteydessä. Keksintöä ei kuitenkaan ole tarkoitus rajoittaa mihinkään tiettyyn tietoliikennejärjestelmään tai tiedonsiirtoprotokollaan. Keksinnön sovellukset myös muihin järjestelmiin ovat alan ammattimiehelle ilmeisiä..

15 Kuviossa 1 on esitetty esimerkki TETRA-järjestelmän rakenteesta. Vaikka kuviossa ja seuraavassa selityksessä on viitattu TETRA-järjestelmän mukaisiin verkkoelementteihin, ei tämä mitenkään rajoita keksinnön soveltamista myös muihin tietoliikennejärjestelmiin. On huomattava, että kuviossa on esitetty vain keksinnön ymmärtämisen kannalta olennaisia elementtejä ja järjestelmän rakenne saattaa poiketa esitetystä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta. On myös huomattava, että todellisessa matkaviestinjärjestelmässä voi kutakin elementtiä olla mielivaltaisen määrä. Päätelaitteet MS (Mobile Station) ovat yhteydessä tukiasemiin TBS (TETRA Base Station) radioteitse. Päätelaitteet MS voivat myös ns. suorakanavamoo-
25 dissa viestiä suoraan keskenään käyttämättä tukiasemia TBS. Jokainen tukiasema TBS on kytketty yhteysjohdolla johonkin kiinteään siirtoverkon TETRA-keskuksista DXT (Digital Exchange for TETRA). TETRA-keskukset DXT on kytketty kiinteällä yhteydellä toisiin keskuksiin ja TETRA-solmukeskukseen DXTc (Digital Central Exchange for TETRA, ei esitetty), joka on keskus, johon
30 on kytketty muita keskuksia DXT ja/tai muita solmukeskuksia DXTc vaihtoehtoisten liikennereittien aikaansaamiseksi. Mahdolliset ulkoiset liitántärajapinnat esimerkiksi yleiseen puhelinverkkoon PSTN (Public Switched Telephone Network), digitaaliseen monipalveluverkkoon ISDN (Integrated Services Digital Network), yritysvaihteeseen PABX (Private Automatic Branch Exchange) ja
35 pakettivälitteiseen dataverkkoon PDN (Packet Data Network) voivat sijaita yhdessä tai useammassa keskuksessa DXT. Edellä mainituista liitántärajapin-

noista on kuviossa esitetty liitanta pakettivälitteiseen dataverkkoon PDN yhdyskäytävän GW avulla. Yhdyskäytävän GW tehtävä on muuttaa keskukselta DXT tuleva piirikytketty data pakettiverkkoon PDN meneväksi pakettikytketyksi dataksi ja päinvastoin. Pakettivälitteiseen dataverkkoon PDN kytketty pääte-

5 laite TE voi näin olla yhteydessä TETRA-verkkoon. Yhdyskäytävä GW voi olla erillinen verkkoelementti tai esimerkiksi keskuksen DXT osa. Lisäksi kuviossa on esitetty keskukseseen DXT kytketty käyttöpaikkajärjestelmä DS (Dispatcher System), joka muodostuu käyttöpaikan ohjaimesta DSC (Dispatcher Station Controller) ja siihen liitetystä työasemasta DWS (Dispatcher Workstation).

10 Käyttöpaikanhoitaja ohjaa päätelaitteiden MS puheluita ja muita toimintoja työaseman DWS välityksellä.

Kuviossa 2 on havainnollistettu päästä-päähän -salauksen toimintaa. Päästä-päähän -salausta käytettäessä lähettäjä 20 koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte (P).

15 Pääte-laite luo P:n pituista avainsarjaa (KSS, Key Stream Segment) avainsarjakehittimessä 21. Salattu näyte (C) saadaan suorittamalla binäärinen XOR-operaatio lohkoissa 22:

$$C = P \text{ xor } KSS$$

20

Salattu näyte lähetetään sitten siirtoverkolle 29. Vastaanottaja 30 suorittaa saman XOR-operaation lohkoissa 28 käyttämällä samaa avainsarjaa, josta syntyy taas selväkielinen näyte P.

$$P = C \text{ xor } KSS$$

25

Salauksen murtamisen ehkäisemiseksi avainsarjaa KSS muutetaan jatkuvasti, joten jokainen kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien 21 ja 27 on siis sovittava siitä, mitä avainsarjaa on käytettävä kullekin kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle 23 ja 26. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

30

Avainsarjakehitin (EKSG, Encryption Key Stream Generator) 21 ja 27 luo avainsarjan (KSS) salausavaimen (CK, Cipher Key) ja alustusvektorin (IV) perusteella. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti.

35

KSS = EKSG (CK, IV)

Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen salausalgoritmi
5 päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salauksen murtamisen ehkäisemiseksi.

Tahdistusohjauksen 23 ja 26 tehtävä on varmistaa, että molemmat päät 20 ja 30 tietävät, millä alustusvektorilla jokainen kehys on salattu. Jotta salaaaja 20 ja avaaaja 30 pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa lähetetään tahdistusvektori (SV). Joskus kyseessä
10 saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikana. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti n. 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden.
15

Vastaanottaja 30 laskee siis kuinka monta kehystä (n) on lähetetty tahdistusvektorin jälkeen. Vastaanottajan 30 avainsarjakehitin 27 luo uuden alustusvektorin IV viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella. Vastaanottajan suorittamaa alustusvektorin IV laskemista
20 on havainnollistettu kuviossa 3, jossa on esitetty siirrettävä kehysjono. Kukin kehys käsittää kaksi puhelohkoa P1 ja P2, kuten kuviossa on esitetty yhden kehyksen osalta. Esitetyssä jonossa kehykset 1, 6, 12 ja 13 sisältävät toisessa puhelohkossaan tahdistusvektorin SV, joissa ilmoitetaan alustusvektorin IV numero.

Molempien päiden 20 ja 30 on sovittava siitä, miten puhelu salataan. Tahdistuksen ohjausyksiköt 23 ja 26 molemmissa päissä kommunikoivat keskenään U-varastettujen puhelohkojen avulla. Lähettävä päätelaite käyttää hyväkseen yhtä tai kahta puhelohkoa kehyksen sisältä omaan tarkoitukseensa. Tämä tapahtuu lohkoissa 24. Tämä ilmaistaan vastaanottavalle päätelaitteelle asettamalla tarkoituksenmukaisesti 3 ensimmäistä ohjausbittä kehyksen sisällä. Siten infrastruktuuri 29 ymmärtää, että kyseessä on päätelaitteesta päätelaitteeseen -tieto, ja se siirtää tietoja sen perusteella läpinäkyvästi muuttamatta niitä. Sen lisäksi vastaanottava päätelaite havaitsee, ettei ko. puhelohkossa ole puhetietoja, eikä välitä niitä koodekille, vaan käsittelee niitä tarkoituksenmukaisesti, toisin sanoen lohkoissa 25 suodatetaan tahdistuksenohjaustieto tahdistuksenohjaukselle 26, ja luo korvaavan äänen varastetun pu-
30
35

heen sijaan. Puhelohkon varastaminen hävittää 30 ms pituisen puheen. Tämä aiheuttaisi tauon puheessa, joten sen laatu huononisi ja sitä olisi vaikeampi ymmärtää. Tämän välttämiseksi TETRA-koodekki sisältää korvausmekanismin. Todellisuudessa käyttäjä ei koe puheen puuttumista haitallisena, mikäli 5 puhelohkoja ei varasteta, enemmän kun 4 kertaa sekunnissa. Salausavaimet CK jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia.

Kuviossa 1 esitetty pakettikytkentäinen dataverkko PDN voi olla esimerkiksi Internet, jossa käytetään TCP/IP protokollia. TCP/IP on tiedonsiir- 10 toprotokollaperheen nimi, jota käytetään lähiverkon sisällä tai lähiverkkojen välillä. Protokollat ovat IP (Internet-protokolla), kuljetusprotokolla TCP (Transmission Control Protocol) ja tietosähkeprotokolla UDP (User Datagram Protocol). Perheeseen kuuluu myös muita protokollia tiettyjä palveluja, kuten tiedostosiirtoa, sähköpostia, etäkäyttöä ym., varten.

15 TCP/IP-protokollat on jaettu kerroksiin: yhteyskerros, verkkokerros, kuljetuskerros ja sovelluskerros. Yhteyskerros vastaa päätelaitteen fyysisestä liittymisestä verkkoon. Se koskee lähinnä verkkokorttia ja ajuria. Verkkokerrosta kutsutaan usein Internet- tai IP-kerrokseksi. Kerros vastaa pakettien siirtämisestä verkon sisällä ja mm. reitityksestä koneesta toiseen IP-osoitteen 20 perusteella. IP tarjoaa TCP/IP-protokollaperheessä verkkokerroksen. Kuljetuskerros tarjoaa datavuopalvelun kahden päätelaitteen välillä sovelluskerrosta varten ja ohjaa vuot päätelaitteessa oikeaan sovellukseen. Internet-protokollassa on kaksi siirtoyhteykäytäntöä: TCP ja UDP. Siirtokerroksen toinen tehtävä on ohjata paketit oikeaan sovellukseen porttinumeroiden perusteella. TCP tarjoaa luotettavan datavuon päätelaitteesta toiseen. TCP pilkkoo 25 datan sopivankokoisiksi paketeiksi, kuittaa vastaanotetut paketit ja valvoo, että lähetetyt paketit kuitataan vastaanotetuiksi toisessa päässä. TCP vastaa luotettavasta siirrosta päästä-päähän, eli sovelluksen ei tarvitse huolehtia siitä. UDP on toisaalta paljon yksinkertaisempi protokolla. UDP ei vastaa tietojen 30 perilletulosta, vaan tätä vaadittaessa sovelluskerroksen on huolehdittava siitä. Sovelluskerros vastaa kunkin sovelluksen omasta tiedonkäsittelystä.

RTP on Internetin standardiprotokolla tosiaikaisen tiedon, kuten äänen ja videokuvan siirtämiseen. Sitä voidaan käyttää mediatilauspalvelua tai vuorovaikutteista palvelua kuten IP-puheluita varten. RTP koostuu media- 35 osasta ja ohjausosasta. Jälkimmäistä kutsutaan RTCP:ksi (Real Time Control Protocol). RTP:n mediaosasta löytyy tukea tosiaikaisille sovelluksille. Tämä si-

sältää aikatuon, kadon havaitsemisen, turvallisuustuen ja sisällön tunnistamisen. RTCP mahdollistaa tosiaikaiset konferenssit erikokoisten ryhmien sisällä ja sen lisäksi päästä-päähän -palvelun laadun arvioinnin. Se tukee myös useamman mediavuon tahdistusta. RTP on suunniteltu siirtoverkosta riippumattomaksi, mutta Internet-verkossa RTP käyttää yleensä IP/UDP:tä. RTP-yhteyskäytännöllä on monia piirteitä, jotka mahdollistavat päästä-päähän tosiaikaisen tiedonsiirron. Jokaisessa päässä audiosovellus lähettää säännöllisesti audiotietoja pieninä näytteinä, jotka voivat olla pituudeltaan esimerkiksi 30 ms. Jokaiseen näytteeseen liitetään RTP-otsikko. RTP-otsikko ja tiedot taas pakataan UDP- ja IP-pakettiin.

RTP-otsikossa tunnistetaan paketin sisältö. Tämän kentän arvoa käyttämällä ilmaistaan, mitä koodausmenetelmää käytetään (PCM, ADPCM, LPC jne.) RTP-paketin hyötykuormassa. Internetissä, kuten muissa pakettiverkoissa, paketit voivat saapua mielivaltaisessa järjestyksessä, myöhästyä vaihtelevan ajan tai jopa kadota kokonaan. Tämän estämiseksi jokaiselle paketille tietyssä vuossa annetaan oma järjestysnumero ja aikaleima, jonka perusteella vastaanotettu vuo järjestyy uudelleen alkuperäisen vuon mukaan. Järjestysnumeroa kasvatetaan yhdellä jokaista pakettia kohti. Järjestysnumeroiden avulla vastaanottaja pystyy havaitsemaan puuttuvan paketin ja myös arvioimaan pakettihukan.

Aikaleima on 32 bittinen numero. Sillä ilmaistaan näytteenoton aloitushetki. Sen laskemiseen on käytettävä monotonisesti ja lineaarisesti ajan mukana kasvavaa kelloa. Kellon taajuus on valittava siten, että se on sisällölle sopiva, tarpeeksi nopea värinän laskemiseksi ja tahdistuksen mahdollistamiseksi. Esimerkiksi käytettäessä PCM-A-laki-koodaustapaa kellotaajuus on 8000 Hz. Lähetettäessä 240-tavun pituisia RTP-paketteja, joka vastaa 240 PCM-näytettä, aikaleimaa kasvatetaan 240:llä jokaista pakettia kohti. RTP-otsikon pituus on 3 - 18 sanaa (32-bittinen sana). Kuviossa 4 on havainnollistettu RTP-paketin muotoa. Kenttien merkitys on seuraava: V: versio; käytetty RTP:n versio, nykyisin 2. Täyte: paketissa on täytetäviä; viimeinen tavu ilmoittaa, montako. Laajennus: paketin jälkeen tasan yksi otsakelaajennus. PM: palvelulähteiden määrä ilmoittaa, monenko lähteen tuottamaa informaatiota paketissa on. Merkitsintä voidaan käyttää ilmoittamaan merkittävistä tapahtumista esimerkiksi kehysten rajoista. HT: hyötykuorman tyyppi ilmoittaa hyötykuormassa olevan median tyyppin. Sarjanumeroa kasvatetaan yhdellä jokaista lähetettyä datapakettia kohti. Se auttaa havaitsemaan pakettihukan ja epäjär-

5 jestyksen. Alkuarvo on satunnainen. Aikaleima kertoo ensimmäisen tavun
 näytteistyshetken. Sitä käytetään tahdistukseen ja värinän laskemiseen. Alku-
 arvo on satunnainen. SSRC: satunnaisesti valittu tahdistuslähteen tunniste.
 Ilmoittaa lähteiden yhdistyspisteen tai alkuperäisen lähettäjän, jos on vain yksi
 lähde. CSRC-lista tässä paketissa mukana olevien lähteiden lista.

10 Internet aiheuttaa vaihtelevan viiveen äänipakettien siirrossa. Pu-
 heen ymmärrettävyyden kannalta viiveen vaihtelu on hyvin haitallista. Tämän
 korvaamiseksi RTP:n vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja
 toistaa ne tiettyyn toisto aikaan. Ennen toistohetkeä tullut paketti osallistuu al-
 kuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut pa-
 ketti on käyttämätön ja hylätty.

15 Kuvio 5 havainnollistaa RTP-algoritmin toimintaa. Kuviossa kirjain t
 viittaa paketin lähetysajankohtaan, kirjain a vastaanottoajankohtaan ja p tois-
 toajankohtaan. Yläindeksit ilmaisevat paketin numeroa ja alaindeksit puheen-
 20 vuoron numeroa. K:nnessä puheenvuorossa paketit saapuvat vastaanotto-
 päähän vaihtelevan siirtoaajan jälkeen. RTP-algoritmi toistaa ne sitten oikealla
 hetkellä. (K+1):nnessä puheenvuorossa paketit 1 ja 2 vaihtelevat järjestystä, ja
 paketti 4 saapuu toistohetkensä jälkeen, joten se hylätään. RTP-algoritmi pa-
 lauttaa paketit oikeaan järjestykseen, toistaa ne oikealla hetkellä, ja ilmaisee
 25 esimerkiksi korjaustoimenpiteitä varten, mitkä paketit puuttuvat tai ovat myö-
 hästyneet. Toistoviive on aika $t(\text{toistoviive}) = t(\text{toisto}) - t(\text{lähetys})$. RTP-
 algoritmi huolehtii siitä, että toistoviive jää vakioksi koko puhevuoron aikana.

30 IP-paketin viive IP-verkon läpi $t = t(\text{tulo}) - t(\text{lähtö})$ koostuu kahdesta
 tekijästä. L on kiinteä viive, joka riippuu siirtoaajasta ja keskimääräisestä jono-
 25 tusajasta. J on taas vaihteleva viive, joka riippuu vaihtelevasta jonotusajasta
 IP-verkon sisällä, ja joka aiheuttaa jitterin. IP-verkon vastaanottopäässä on jit-
 terpuskuri, joka tallentaa paketit muistiinsa, mikäli siirtoaika $t < t(\text{toistoviive})$.
 Toistoviiveen määrittäminen on kompromissiratkaisu. Tosiaikainen sovellus
 vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halu-
 30 taan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan paket-
 tien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistovii-
 veen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Kuvio
 6 havainnollistaa tätä. Paketti, jonka siirtoaika $t < L + J$ voidaan hyväksyä, kun
 taas paketti, jonka siirtoaika $t > L + J$ on hylättävä. Kasvattamalla J:tä voidaan
 35 näin kasvattaa hyväksytyjen pakettien määrää. Toistoviivettä voidaan säätää

esimerkiksi aloittamalla pienellä arvolla, ja kasvattamalla sitä säännöllisesti, kunnes myöhässä olevien pakettien osa jää tietyn rajan, esimerkiksi 1%, alle.

Useimmilla RTP-algoritmeilla on toiminne, joka säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi.

- 5 Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että RTP-vastaanotossa luodaan 60 ms:n korvaava puhepaketti ennen kun puhe-
vuo jatkuu. Toisin sanoen lisätään puhevuon sisälle ylimääräinen kehys. Kuvi-
ossa 7 on esitetty kehysjono 75, johon lisätään yksi tai useampia ylimääräisiä
kehysjä 72 ja edelleentoimitusta varten saadaan kehysjono 76. Toistoviiveen
10 siirtäminen 60 ms taaksepäin tapahtuu puolestaan siten, että RTP-
vastaanotossa kokonainen puhekehys hävitetään.

- Kuviossa 1 RTP-siirto tapahtuu siis yhdyskäytävän GW ja pääte-
laitteen TE välillä pakettiverkon PDN yli. Yhdyskäytävän GW tehtävä on
muuntaa keskukselta DXT PCM-linjaa pitkin tuleva piirikytketty puhe (tai muu
15 data) IP-puhepaketeiksi ja päinvastoin. TETRA-infrastruktuurissa siirretään
puhedataa kehyksissä, joten luonnollinen RTP-paketti sisältäisi yhden kehyk-
sen puhedataa. Tällöin yhdessä RTP-paketissa olisi 60 ms puhetta, ja se
vastaisi suoraan yhden puhekehysten sisältöä. Toinen mahdollisuus on käyt-
tää RTP-pakettia, joka sisältää vain puolikehysten puhedataa (30 ms). Puoli-
20 kehyspaketilla on seuraavat ominaisuudet verrattuna kokonaiskehyspakettiin:
1) Yhdyskäytävän vastaanottaessa puolikehyspaketteja sen täytyy odottaa,
että kaksi pakettia on saapunut ennen ISI-kehysten lähetyksen alkua. Molem-
pia puhelohkoja koskevat ohjausbitit (BFI, C- tai U-varkaus) ovat nimittäin ke-
hyksen alussa ja yhdyskäytävän täytyy määritellä ne puolikehyspakettien tyy-
25 pin perusteella. 2) RTP-paketin kadotessa vain 30 ms puhetta puuttuu verrat-
tuna 60 ms:in. Äänen laatua optimoitaessa on paketin pituus kompromissi
kahden hahmottamisnäkökohdan välillä. Toinen ääripää on lyhyt paketti, jonka
seurauksena puuttuvien pakettien määrä kasvaa kääntäen verrannollisesti pa-
kettien kokoon, ja vääristymät tapahtuvat näin useammin. Toinen ääripää on
30 pitkä paketti, jolloin vääristymät tapahtuvat harvemmin mutta jolla todennäköi-
syys kokonaisen foneemin häviämisestä ja näin ollen puheen ymmärrettävyy-
den huononemisesta kasvaa varsinkin kun paketin pituus on yli 20 ms. Jäl-
kimmäinen raja on nimittäin lyhyin foneemin pituus. 3) Kaistanleveyden kan-
nalta pitkä paketti on kuitenkin tehokkaampi, sillä otsikoiden (Ethernet + IP +
35 UDP + RTP) pituus (36-40 tavua) on hyötykuorman pituuteen verrattuna (18
tavua/puhelohko tai 36 tavua/puhekehys) jo pitkä. Otsikoiden osuutta paketi-

sa voidaan pienentää käyttämällä kahta tekniikkaa. Multipleksauksen avulla voidaan useita puhekanavia pakata samaan RTP-pakettiin ja näin pienentää otsikoiden osuutta. Tämä on varsin kiinnostavaa keskuksesta-käyttöpaikkaan-yhteyttä varten, sillä kaikki ryhmäpuhelut ja yksilöpuhelu voidaan näin lähettää samassa paketissa. Toinen tekniikka, joka soveltuu sarjayhteyksiin, on otsikoiden kompressio. Sen avulla voidaan IP/UDP/RTP-otsikkoa pienentää huomattavasti (2-4 tavuihin) ja näin säästää kaistanleveyttä. Paremman äänenlaadun saavuttamiseksi on lyhyt RTP-paketti (30 ms) näin ollen edullisempi.

Puhelohkoja voidaan varastaa kehyksen sisältä joko verkon (C-varastettu) tai käyttäjän (U-varastettu) tarkoitukseen. Esimerkiksi päästöpäähän -salausta käytettäessä päätelaitteet varastavat yhden puhelohkon omaan tarkoitukseensa 1 - 4 kertaa sekunnissa tahdistusvektorin välittämiseen kuten edellä on selitetty.

ACELP-koodekkeja tuetaan RTP-standardissa ja monessa IP-puhepätelaitteessa, mutta TETRA-kohtaista ACELP:iä ei RTP-standardi tue. Puhkeen siirtämistä varten voidaan käyttää RTP-pakettia, jossa on esimerkiksi seuraavat asetukset: RTP-versio 2, ei täytettä, ei laajennusta, ei CRSC lähteitä, ei merkitsintä, kuorman tyyppi: 8 (sama kuin A-laki), aikaleima kasvaa 240 yksiköllä jokaista pakettia kohti. Tämä vastaa TETRA:n 8000 Hz näytteenottokelloa ja 30 ms näytteenpituutta. Hyötykuormassa esiintyvät seuraavat tiedot: kolme ensimmäistä bittiä ilmaisevat, onko kehysvirhebitti (BFI) asetettu, onko hyötykuormassa ääni vai data, ja onko mahdollisesti kyseessä C- tai U-varastettu puhelohko; muut ensimmäisen tavun bitit eivät ole käytössä; seuraavat 137 bittiä ovat varsinaista dataa, ja ne vastaavat yhtä puhelohkoa. Hyötykuorman loput bitit ovat 0.

Edellä kuvattu yhdyskäytävän GW toiminta piiriytketyn ja pakettiytketyn yhteyden välillä on vain eräs mahdollinen toteutustapa ja yhdyskäytävän GW toiminta voi poiketa tästä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta.

Kuviossa 1 esitetty päätelaite TE voi olla puhepätelaite tai datapätelaite ja keksintöä voidaan soveltaa esimerkiksi ääniyhteyksiin, kuvayhteyksiin tai datayhteyksiin, jotka vaativat reaaliaikaista tiedonsiirtoa. Päätelaite TE voi olla esimerkiksi matkaviestin, käyttöpaikan työasema, tukiasema tai jokin muu verkkoelementti. Päätelaite TE ei ole välttämättä suoraan kytketty pakettiverkkoon PDN vaan päätelaitteen TE ja pakettiverkon PDN välillä voi olla esimerkiksi toinen TETRA-verkko. Tällöin myös pakettiyhteyden PDN toisessa

päässä on yhdyskäytäväelementti. Välissä voi olla myöskin jokin muu yhteys tai useampia pakettiyhteyksiä. Jos päätelaite TE on kuvion 1 mukaisesti kytetty suoraan pakettiverkkoon PDN, toimii se RTP-siirron toisena osapuolena olennaisesti samalla tavoin, kuin jo edellä on kuvattu yhdyskäytävän GW osalta.

Keksinnön mukaisesti suoritetaan pakettiyhteyden PDN vastaanottavassa päässä GW tai TE toistoviiveen kasvatus tiedon lähetyksen, esimerkiksi puheenvuoron tai puhelun, aikana, siten, että merkitään toistoviiveen kasvattamiseksi lisättävä kehys 72 ylimääräiseksi kehykseksi ja edelleen tietoliikenneyhteyden vastaanottavassa päässä lasketaan vastaanotettujen kehysten lukumäärään n vain ylimääräiseksi merkitsemättömät kehykset, jotta oikea alustusvektorin arvo saadaan selville kuten edellä on selitetty. Esimerkinä voidaan tarkastella tilannetta, jossa kuviossa 1 matkaviestimen MS ja päätelaitteen TE välillä on puhelu, joka kulkee pakettiyhteyden PDN kautta RTP-protokollan mukaisesti. RTP-protokollan mukainen tiedonsiirto tapahtuu tällöin protokollaa tukevien yhdyskäytävän GW ja päätelaitteen TE välillä. Tällöin yhdyskäytävä GW on pakettiyhteyden PDN vastaanottava pää päätelaitteelta TE tulevan liikenteen suhteen. Kun RTP-algoritmin mukaisesti havaitaan tarve kasvattaa toistoviivettä, lisätään yhdyskäytävässä GW yksi tai useampia ylimääräisiä kehyksiä 72 vastaanotettuun kehysjonoon 75 ja lähetetään näin saatu kehysjono 76 edelleen matkaviestimelle MS. Lisättävät ylimääräiset kehykset 72 lisäksi merkitään yhdyskäytävässä GW siten, että vastaanottaja eli tässä tapauksessa matkaviestin MS tunnistaa ne ylimääräisiksi kehyksiksi eikä laske niitä mukaan vastaanotettujen kehysten lukumäärään n . Tällöin matkaviestimen MS salausalgoritmi pysyy oikeassa tahdissa. Vastaavalla tavalla päätelaite TE, joka on pakettiyhteyden PDN vastaanottava pää matkaviestimeltä MS tulevan liikenteen suhteen, merkitsee toistoviiveen kasvattamiseksi mahdollisesti lisättävät ylimääräiset kehykset 72. Tällöin seuraavaksi salauksen purkuun ja toistettavaksi edelleensirrettävästä kehysjonosta pystytään päätelaitteen TE salauksen purussa erottamaan ylimääräiset kehykset, joita ei lasketa mukaan vastaanotettujen kehysten lukumäärään n . Toistoviiveen ohjaus päätelaitteessa TE tapahtuu siis kuvion 2 kaavioon viitaten ennen suodatinlohkoa 25. Toistoviiveen kasvattamiseksi lisättävä kehys voidaan merkitä ylimääräiseksi kehykseksi jollakin ennalta sovitulla tavalla. Tapa, jolla merkintä tehdään, ei ole merkityksellinen keksinnön perusajatuksen kannalta. Tärkeintä on, että tietoliikenneyhteyden vastaanottava osapuoli pystyy tunnistamaan

ylimääräiset kehykset. Merkintä voidaan tehdä esimerkiksi käyttämällä erityistä tähän tarkoitukseen varattua parametria, joka välitetään ylimääräisen kehyksen 72 toisessa puhelohkossa, joka on C-varastettu. Merkintä voidaan tehdä jokaiseen ylimääräiseen kehykseen tai jos lähetetään useita ylimääräisiä kehyksiä peräkkäin, on myös mahdollista, että merkintä on vain ensimmäisessä
5 ylimääräisessä kehyksessä ja samalla ilmoitetaan sitä seuraavien ylimääräisten kehysten lukumäärä.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.
10

Patenttivaatimukset

1. Menetelmä päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, jossa määritetään tietoliikenneyhteyden vastaanottavassa päässä vastaanotettujen kehysten lukumäärän perusteella vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävä kehystä vastaava alustusvektorin arvo, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä, jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä siirrettävään kehysjonoon, t u n n e t t u siitä, että

merkitään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi ja

lasketaan vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

toistoviiveen kasvatus suoritetaan pakettikytketyn yhteyden vastaanottavassa päässä.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että pakettikytketty yhteys käyttää Internet-protokollaa.

4. Patenttivaatimuksen 1, 2 tai 3 mukainen menetelmä, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

5. Jonkin patenttivaatimuksista 1–4 mukainen menetelmä, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys käsittää varastetun puhelohkon, jolloin mainittu merkintä tehdään varastettuun puhelohkoon.

6. Jonkin patenttivaatimuksista 1–5 mukainen menetelmä, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

7. Järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin järjestely käsittää

välineet (MS, TE) tietoliikenneyhteyden vastaanottavassa päässä vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon määrittämiseksi vastaanotettujen kehysten lukumäärän perusteella, t u n n e t t u siitä, että järjestely käsittää li-

5 säksi

välineet (GW, TE) toistoviiveen säätämiseksi, jotka on sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehukseksi, jolloin välineet (MS, TE) alustusvektorin arvon määrittämiseksi on sovitettu laskemaan vastaanotettujen kehysten lukumäärään vain ylimääräi-

10 seksi merkitsemättömät kehykset.

8. Patenttivaatimuksen 7 mukainen järjestely, t u n n e t t u siitä, että välineet (GW, TE) toistoviiveen säätämiseksi sijaitsevat pakettikytketyn yhteyden (PDN) vastaanottavassa päässä.

9. Patenttivaatimuksen 7 tai 8 mukainen järjestely, t u n n e t t u siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

10. Patenttivaatimuksen 7, 8 tai 9 mukainen järjestely, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

11. Jonkin patenttivaatimuksista 7–10 mukainen järjestely, t u n n e t t u siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin välineet (GW, TE) toistoviiveen säätämiseksi on sovitettu tekemään mainittu merkintä varastettuun puheloh-

25 koon.

12. Jonkin patenttivaatimuksista 7–11 mukainen järjestely, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

13. Verkkoelementti päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, jossa määritetään tietoliikenneyhteyden vastaanottavassa päässä vastaanotettujen kehysten lu-

30 kumäärän perusteella vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävä kehystä vastaava alustusvektorin arvo, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin verkkoelementti (GW, TE) on sovitettu tarvittaessa kasvattamaan siirrettävän tiedon toistoviivettä lisäämällä yhden tai useampia ylimääräisiä ke-

35 hyksiä (72) siirrettävään kehysjonoon (75), t u n n e t t u siitä, että

verkkoelementti on lisäksi sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi.

14. Patenttivaatimuksen 13 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti sijaitsee pakettikytketyn yhteyden (PDN) vastaanottavassa päässä.

15. Patenttivaatimuksen 13 tai 14 mukainen verkkoelementti, tunnettu siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin verkkoelementti on sovitettu tekemään mainittu merkintä varastettuun puhelohkoon.

16. Patenttivaatimuksen 13, 14 tai 15 mukainen verkkoelementti, tunnettu siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

17. Jonkin patenttivaatimuksista 13–16 mukainen verkkoelementti, tunnettu siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

18. Jonkin patenttivaatimuksista 13–17 mukainen verkkoelementti, tunnettu siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

19. Patenttivaatimuksen 17 tai 18 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on TETRA käyttöpaikan työasema.

20. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on tukiasema.

21. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on mediayhdyskäytävä.

22. Verkkoelementti, joka käyttää tietoliikenneyhteyttä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistovii-vettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin

verkkoelementti (TE, MS) on sovitettu määrittämään vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon vastaanotettujen kehysten lukumäärän perusteella, tunnettu siitä, että

verkkoelementti on lisäksi sovitettu, kun toistoviiveen kasvattamiseksi lisättävät kehykset on merkitty ylimääräisiksi kehyksiksi, laskemaan

vastaanotettujen kehysten lukumäärään vain kehykset, joita ei ole merkitty ylimääräisiksi.

23. Patenttivaatimuksen 22 mukainen verkkoelementti, tunnettu siitä, että toistoviiveen kasvattamiseksi lisättävä ylimääräinen kehys (72) käsittää varastetun puhelohkon, jolloin mainittu merkintä on varastetussa puhelohkossa.

24. Patenttivaatimuksen 22 tai 23 mukainen verkkoelementti, tunnettu siitä, että pakettikytketty yhteys (PDN) käyttää Internet-protokollaa.

10 25. Patenttivaatimuksen 22, 23 tai 24 mukainen verkkoelementti, tunnettu siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

26. Jonkin patenttivaatimuksista 22–25 mukainen verkkoelementti, tunnettu siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

15 27. Patenttivaatimuksen 25 tai 26 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on TETRA käyttöpaikan työasema.

28. Jonkin patenttivaatimuksista 22–26 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on tukiasema.

20 29. Jonkin patenttivaatimuksista 22–26 mukainen verkkoelementti, tunnettu siitä, että verkkoelementti on matkaviestin.

(57) Tiivistelmä

Menetelmä ja järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä (72) siirrettävään kehysjonoon (75), jolloin järjestely käsittää välineet (MS, TE) tietoliikenneyhteyden vastaanottavassa päässä vastaanotetun kehyksen salauksen purkamisessa kulloinkin käytettävän kehystä vastaavan alustusvektorin arvon määrittämiseksi vastaanotettujen kehysten lukumäärän perusteella ja välineet (GW, TE) toistoviiveen säätämiseksi, jotka on sovitettu merkitsemään toistoviiveen kasvattamiseksi lisättävä kehys ylimääräiseksi kehykseksi, jolloin välineet (MS, TE) alustusvektorin arvon määrittämiseksi on sovitettu laskemaan vastaanotettujen kehysten lukumäärään vain ylimääräiseksi merkitsemättömät kehykset.

(Kuvio 1)

Fig. 1

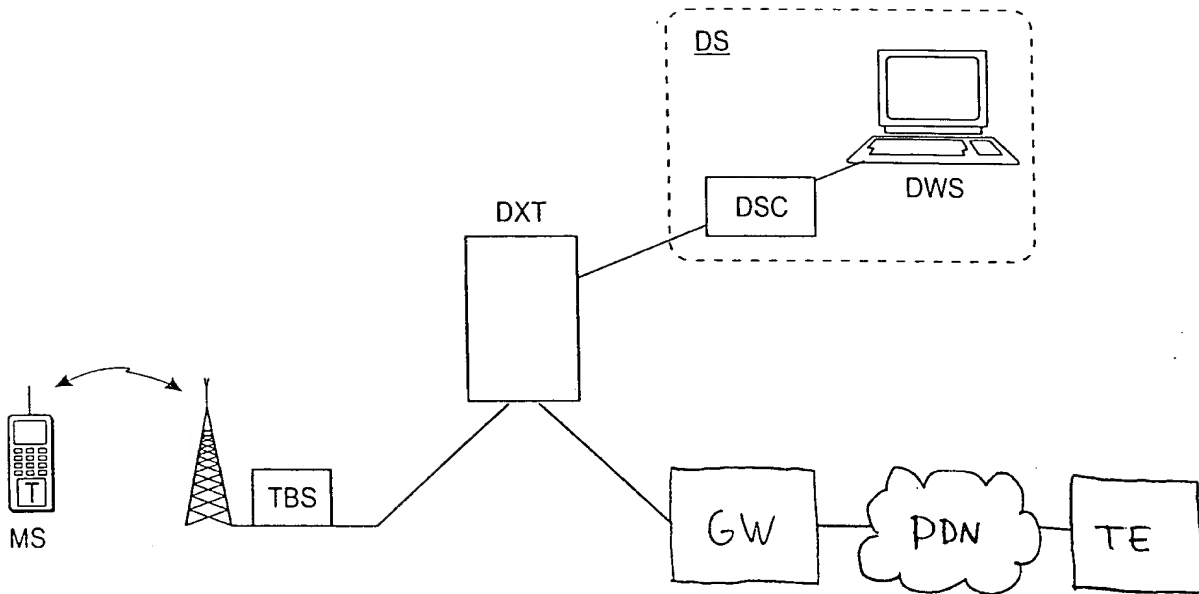
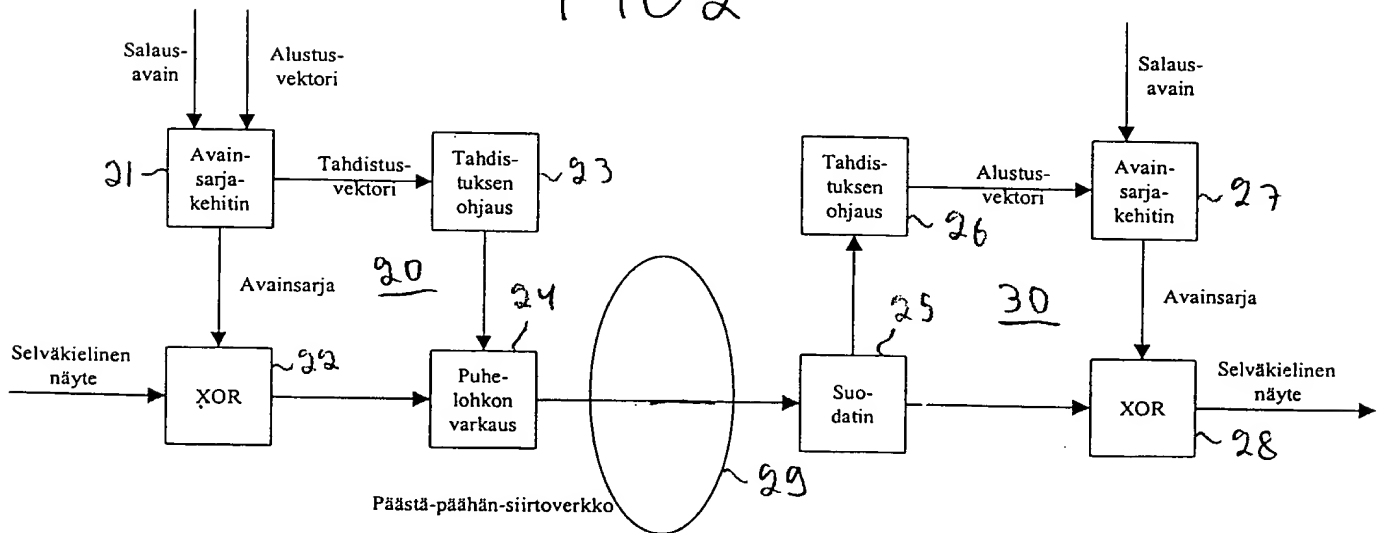


FIG 2



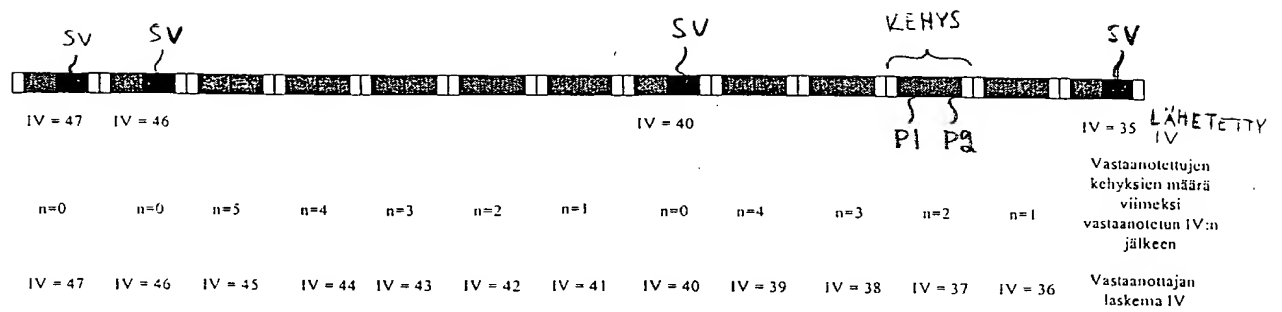


FIG3

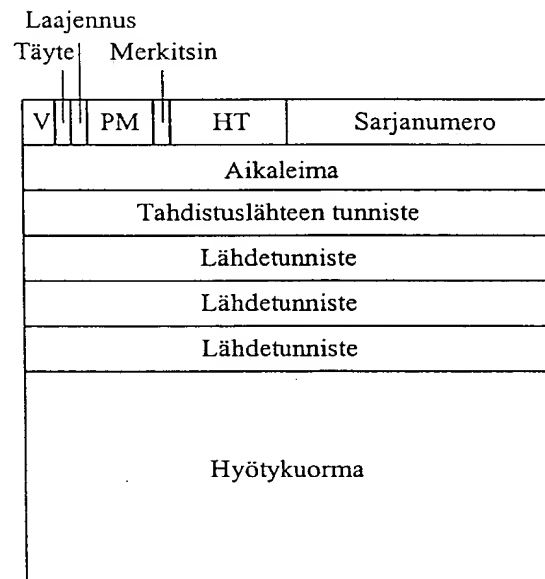


FIG4

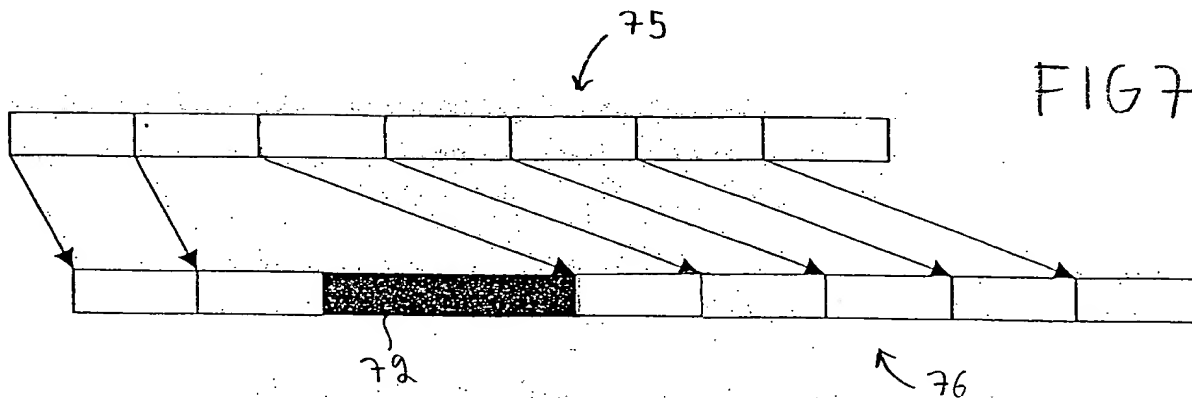


FIG7

FIG 5

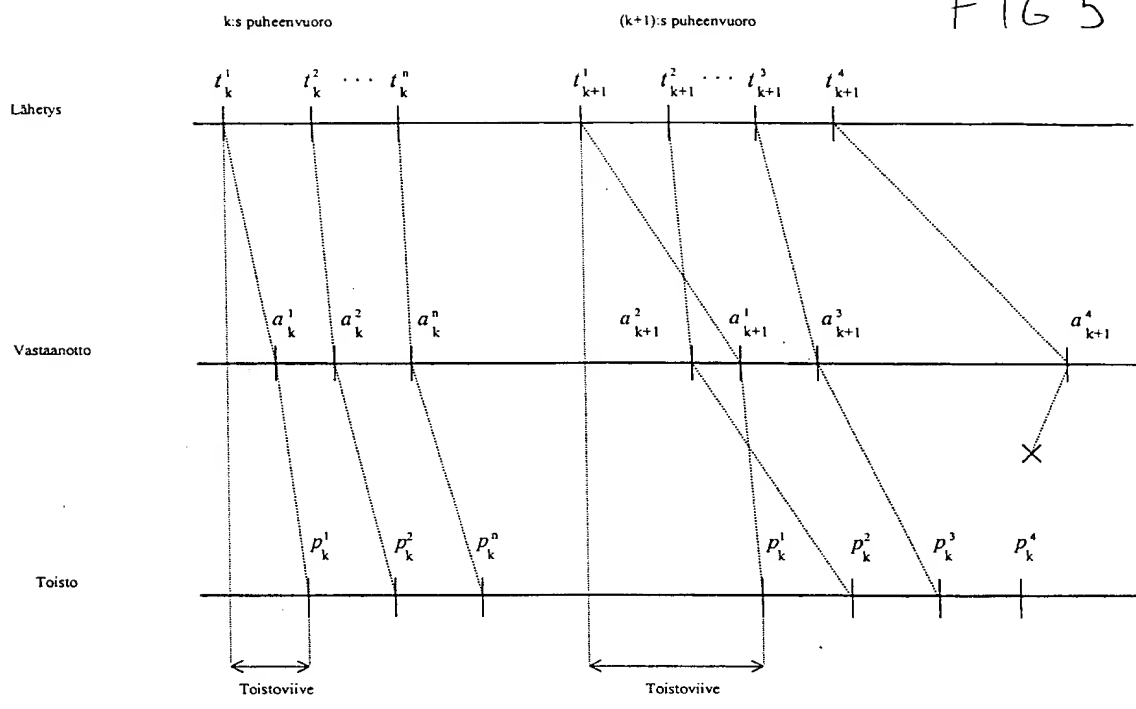


FIG 6

